UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,329	06/27/2001	Marcus Peinado	MSFT-164268.1	1912

41505 7590 11/02/2004

WOODCOCK WASHBURN LLP
ONE LIBERTY PLACE - 46TH FLOOR
PHILADELPHIA, PA 19103

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 11/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PPA

Office Action Summary	Application No.	Applicant(s)	
	09/892,329	PEINADO ET AL.	
	Examiner	Art Unit	
	Eleni A Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/01/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-46 are presented for examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 28 and 44 are rejected under 35 U.S.C. 102(b) as being anticipated by Mario, Fr. et al. (Marino, Patent Number: 5,029,206).

3.1 As per claim 28, Marino teaches a method for a secure processor to instantiate a secure application thereon (Marino Abstract), the method comprising:

instantiating a first security kernel which employs symmetric cryptography (Marino Col. 6 lines 48-57, col. 1 lines 50-63);

instantiating by way of the instantiated first security kernel a second security kernel which employs asymmetric cryptography (Marino col. 9 lines 27-39, col. 1 lines 50-63); and

authenticating by way of the instantiated second security kernel the secure application (Marino Col. 6 lines 48-57, col. 10 lines 5-26).

3.2 As per claim 44, Marino teaches a computer-readable medium having stored thereon computer-executable instructions implementing a method for a secure processor to instantiate a secure application thereon, the method comprising:

instantiating a first security kernel which employs symmetric cryptography (Marino Col. 6 lines 48-57, col. 1 lines 50-63);

instantiating by way of the instantiated first security kernel a second security kernel which employs asymmetric cryptography (Marino col. 9 lines 27-39, col. 1 lines 50-63); and

authenticating by way of the instantiated second security kernel the secure application (Marino Col. 6 lines 48-57, and col. 10 lines 5-26).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-2, 4, 6, 7, 9-20, 27, 31-36, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marino Jr. et al. (Marino, US Patent Number: 5,029,206) in view of Angelo et al. (Angelo, US Patent Number: 6,581,162 B1)

5.1 As per claim 1, Marino teaches a secure processor for a computing device,

the processor including a security kernel for being instantiated on the processor when the processor enters into the preferred mode (Marino Col. 3 lines 45-58) and

a security key accessible by the instantiated security kernel when the processor is operating in the preferred mode (Marino Col. 4 lines 27-38; security kernel encryption key),

the security kernel employing the accessed security key during the preferred mode to authenticate a secure application on the computing device (Marino Col. 6 lines 48-57),

wherein the security kernel allows the processor to be trusted to keep hidden a secret of the application (Marino Col. 9 lines 49-58, and abstract),

Marino does not explicitly teach the processor being operable in a normal mode and a preferred mode,

However Angelo teaches in a computer system a method for securely managing encryption information, having a secure mode of operation and a normal mode of operation (Angelo Col. 10 lines 53-56) that reads on the processor being operable in a normal mode and a preferred mode.

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Angelo with in the system of Marino because it would allow to operate a processor of a computer system in the normal mode to store normal software processes in a normal memory space accessible by a general processor of the computer system, and perform normal computer operation in the normal memory space; and in a preferred mode (secure mode) to store the encryption algorithm in a secure memory space not accessible to the normal software processes and only accessible by the general processor in the secure mode of

operation, receive encryption information in the secure memory space through a secure channel, store encryption information in the secure memory space and perform an encryption process only in the secure memory space with encryption information (Angelo Col. 10 lines 57-Col. 11 lines 9).

5.2 As per claim 15, Marino teaches a method for a secure processor to instantiate and authenticate a secure application thereon by way of a security kernel, the method comprising:

entering a preferred mode where a security key of the processor is accessible (Marino Col. 3 lines 43-58, col. 4 lines 27-38);

instantiating and running a security kernel, the security kernel (Marino Col. 3 lines 43-58): accessing the security key (Marino Col. 1 lines 50-63);

applying the accessed security key to decrypt at least one encrypted key for the application (Marino Col. 2 lines 3-10, col. 3 lines 26-33);

storing the decrypted key(s) in a location where the application will expect the key(s) to be found (Marino Col. 3 lines 12-25); and

authenticating the application on the processor (Marino Col. 6 lines 48-58); and

wherein the security kernel allows the processor to be trusted to keep hidden the key(s) of the application (Marino Abstract, and Col. 3 lines 12-25).

Marino does not explicitly teach entering a normal mode from the preferred mode after the security kernel authenticates the application, where the security key is not accessible;

However Angelo discloses entering a normal mode from the preferred mode after the security kernel authenticates the application, where the security key is not accessible (Angelo Col. 3 lines 5-23);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Angelo with in the system of Marino because it would allow to operate a processor of a computer system in the normal mode to store normal software processes in a normal memory space accessible by a general processor of the computer system, and perform normal computer operation in the normal memory space; and in a preferred mode (secure mode) to store the encryption algorithm in a secure memory space not accessible to the normal software processes and only accessible by the general processor in the secure mode of operation, receive encryption information in the secure memory space through a secure channel, store encryption information in the secure memory space and perform an encryption process only in the secure memory space with encryption information (Angelo Col. 10 lines 57-Col. 11 lines 9) and information maintained in a secure memory space is not accessible during a normal computer operation (Angelo Col. 3 lines 5-23). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to enter a normal mode from the preferred mode because it would exit access from the preferred mode and perform a normal operation with out accessing information maintained in a secure memory space and enhance security.

5.3 As per claim 31, Marino teaches a computer-readable medium having stored thereon computer-executable instructions implementing a method for a secure processor to instantiate a secure application thereon by way of a security kernel, the method comprising:

entering a preferred mode where a security key of the processor is accessible (Marino Col. 3 lines 43-58, col. 4 lines 27-38);

instantiating and running a security kernel, the security kernel (Marino Col. 3 lines 43-58): accessing the security key (Marino Col. 1 lines 50-63);

applying the accessed security key to decrypt at least one encrypted key for the application (Marino Col. 2 lines 3-10, col. 3 lines 26-33);

storing the decrypted key(s) in a location where the application will expect the key(s) to be found (Marino col. 3 lines 12-25); and

authenticating the application on the processor (Marino Col. 6 lines 48-58);

security kernel authenticates the application (Marino Col. 6 lines 48-57); and

wherein the security kernel allows the processor to be trusted to keep hidden the key(s) of the application (Marino Abstract, and col. 3 lines 12-25)

Marino does not explicitly teach entering a normal mode from the from the preferred mode after the security kernel authenticates the application, where the security key is not accessible;

However Angelo discloses entering a normal mode from the preferred mode, where the security key is not accessible (Angelo Col. 3 lines 5-23);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Angelo with in the system of Marino because it would allow to operate a processor of a computer system in the normal mode to store normal software processes in a normal memory space accessible by a general processor of the computer system, and perform normal computer operation in the normal memory space; and in a preferred mode (secure mode) to store the encryption algorithm in a secure memory space not accessible to the normal software processes and only accessible by the general processor in the secure mode of operation, receive encryption information in the secure memory space through a secure channel, store encryption information in the secure memory space and perform an encryption process only in the secure memory space with encryption information (Angelo Col. 10 lines 57-Col. 11 lines 9) and information maintained in a secure memory space is not accessible during a normal computer operation (Angelo Col. 3 lines 5-23). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to enter a normal mode from the preferred mode after the security kernel authenticates the application where the security key is not accessible because it would exit access from the preferred mode and perform a normal operation with out accessing security key and information maintained in a secure memory space and enhance security.

5.4 As per claim 2, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches the processor in combination with the application (Marino Col. 1 lines 20-39).

5.5 As per claim 4, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches the processor wherein the security kernel automatically authenticates a particular application (Marino Col. 4 lines 27-48).

5.6 As per claim 6, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches the processor wherein the security kernel employs the accessed security key during the preferred mode to decrypt at least one encrypted key for the application (Marino Col. 3 lines 26-33).

5.7 As per claim 7, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches the processor in combination with the computing device (Marino Col. 5 lines 52-58; encryption device).

5.8 As per claim 9, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches the processor further comprising a storage space, the security kernel being permanently stored in the storage space (Marino Col. 3 lines 12-25).

5.9 As per claim 10, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches the processor further comprising a storage space, the security key being permanently stored in the storage space (Marino Col. 12 lines 53-60, claim 10)

5.10 As per claim 11, Marino and Angelo teach all the subject matter as described above. In

addition Marino teaches the processor wherein the security kernel employs the accessed security key during the preferred mode to authenticate/verify the application prior to instantiation thereof (Marino Col. 9 lines 27-col. 10 lines 26).

5.11 As per claim 12, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches the processor wherein the security kernel performs a hash/MAC (message authentication code) over at least a portion of the application and then compares the hash/MAC to a hash/MAC corresponding to the application (Marino Col. 9 lines 27-col. 10 lines 26).

5.12 As per claim 13, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches the processor wherein such processor enters preferred mode whenever a predefined initializing processor action is performed (Marino Col. 8 lines 58-69).

5.13 As per claim 14, Marino and Angelo teach all the subject matter as described above. In addition Angelo teaches the processor wherein such processor enters preferred mode whenever a CPU reset is performed (Angelo Col. 3 lines 5-24). The rational for combining are the same as claim 15 above.

5.14 As per claim 16 and 32, Marino and Angelo teach all the subject matter as described above. In addition Angelo teaches the method (medium) wherein entering the preferred mode comprises entering the preferred mode upon a CPU reset (Angelo Col. 3 lines 5-23). The rational

for combining are the same as claim 15 above.

5.15 As per claim 17 and 33, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches a method (medium) further comprising erasing data in a cache of the processor prior to instantiating the security kernel (Marino Col. 10 lines 40-68). The rational for combining are the same as claim 15 above.

5.16 As per claim 18 and 34, Marino and Angelo teach all the subject matter as described above. In addition Angelo teaches a method (medium) further comprising erasing data in a cache of the processor after entering normal mode (Angelo Col. 7 lines 27-40).

5.17 As per claim 19 and 35, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches a method (medium) wherein the security kernel employs the accessed security key during the preferred mode to authenticate/verify the application prior to instantiation thereof (Marino Col. 9 lines 27-col. 10 lines 26).

5.18 As per claim 20 and 36, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches a method (medium) wherein the security kernel performs a hash/MAC (message authentication code) over at least a portion of the application and then compares the hash/MAC to a hash/MAC corresponding to the application (Marino Col. 9 lines 27-col. 10 lines 26).

5.19 As per claim 27 and 43, Marino and Angelo teach all the subject matter as described above. In addition Marino teaches a method (medium) further comprising storing the chooser value in a memory location not affected by a CPU reset so that the stored chooser value is available after same (Angelo Col. 3 lines 5-23). The rational for combining are the same as claim 15 above.

6. Claims 3, 5, 21-26, 29-30, 37-42, and 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marino Jr. et al. (Marino, US Patent Number: 5,029,206) in view of Angelo et al. (Angelo, US Patent Number: 6,581,162 B1), and in further view of Downs et al. (Downs US Patent No. 6,574,409 B1).

6.1 As per claim 25, Marino teaches a method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel, the method comprising:

instantiating the security kernel (Marino Col. 1 lines 50-63),

the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application (Marino abstract, and col. 3 lines 12-25)

Marino does not explicitly teach setting a value upon power-up;

entering a preferred mode upon a power-up CPU reset and determining that the chooser value corresponds to the chooser application and therefore authenticating same, the chooser application being instantiated;

entering a normal mode after the chooser application is instantiated and leaving same to run, the chooser application presenting the plurality of available applications for selection by a user;

entering a preferred mode upon an executed CPU reset and determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated;

entering a normal mode after the selected application is instantiated and leaving same to run;

However Angelo discloses setting a value upon power-up (Angelo Col. 3 lines 5-23; user information entered during secure mode is protected upon power-up);

entering a preferred mode upon a power-up CPU reset (Angelo Col. 3 lines 5-23, and col. 3 lines 33-40) and determining that the chooser value corresponds to the chooser application and therefore authenticating same, the chooser application being instantiated (Angelo Col. 9 lines 64-col. 10 lines 11);

entering a normal mode after the chooser application is instantiated and leaving same to run (Angelo Col. 3 lines 5-23; information is not accessible during the normal computer operation);

entering a preferred mode upon an executed CPU reset (Angelo Col. 3 lines 5-23, and col. 3 lines 33-40) and determining that the chooser value corresponds to the selected application

and therefore authenticating same, the selected application being instantiated (Angelo Col. 9 lines 64-col. 10 lines 11);

entering a normal mode after the selected application is instantiated and leaving same to run (Angelo Col. 3 lines 5-23; information is not accessible during the normal computer operation);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Angelo with in the system of Marino because it would provide a secure environment from which to verify files (Angelo Col. 9 lines 64-col. 10 lines 11). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ Angelo's teaching with in the system of Marino because it would set a chooser value to a value corresponding to a chooser application upon power-up. Upon power-up or reset, the computer performs the power on self-test by verifying and comparing hash value to a value stored. Loading information in to memory and execution is performed after integrity is verified.

Mario and Angelo do not explicitly teach a chooser value to a value corresponding to a chooser application;

the chooser application presenting the plurality of available applications for selection by a user;

receiving a selection of one of the presented applications to be instantiated; and

setting the chooser value to a value corresponding to the selected application;

However Downs teach setting a chooser value to a value corresponding to a chooser application (Downs Col. 31 lines 60-67, and Col. 83 lines 43-64 a user makes a selection of a digital content among a plurality of digital contents and the selected value is set and music is stored in users device)

the chooser application presenting the plurality of available applications for selection by a user (Downs col. 28 lines 4-7; Content ID is used to uniquely identify content among plurality of contents);

receiving a selection of one of the presented applications to be instantiated (Downs Col. 25 lines 16-22, col. 77 lines 5-23);

setting the chooser value to a value corresponding to the selected application (Downs Col. 31 lines 60-67, and Col. 83 lines 43-64);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Downs with in the combination system of Marino and Angelo because it would securely deliver digital contents and rights management of digital assets such as print media, films games, and music over global communications networks (Downs Col. 1 lines 61-67) by encrypting content data with a first encryption key and encrypting the first encryption key with a second encryption key (Downs Col. 3 lines 49-67).

6.2 As per claim 41, Marino teaches a computer-readable medium having computer-executable instructions thereon implementing a method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel, the method comprising:

instantiating the security kernel (Marino Col. 1 lines 50-63)

the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application (Marino abstract, and col. 3 lines 12-25);

Marino does not explicitly teach setting a value upon power-up;

entering a preferred mode upon a power-up CPU reset and determining that the chooser value corresponds to the chooser application and therefore authenticating same, the chooser application being instantiated;

entering a normal mode after the chooser application is instantiated and leaving same to run, the chooser application presenting the plurality of available applications for selection by a user;

entering a preferred mode upon an executed CPU reset and determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated;

entering a normal mode after a selected application is instantiated and leaving same to run;

However Angelo discloses setting a value upon power-up (Angelo Col. 3 lines 5-23; user information entered during secure mode is protected upon power-up);

entering a preferred mode upon a power-up CPU reset (Angelo Col. 3 lines 5-23, and col. 3 lines 33-40) and determining that the chooser value corresponds to the chooser application and

therefore authenticating same, the chooser application being instantiated (Angelo Col. 9 lines 64-col. 10 lines 11);

entering a normal mode after the chooser application is instantiated and leaving same to run (Angelo Col. 3 lines 5-23; information is not accessible during the normal computer operation);

entering a preferred mode upon an executed CPU reset (Angelo Col. 3 lines 5-23, and col. 3 lines 33-40) and determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated (Angelo Col. 9 lines 64-col. 10 lines 11);

entering a normal mode after the selected application is instantiated and leaving same to run (Angelo Col. 3 lines 5-23; information is not accessible during the normal computer operation);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Angelo with in the system of Marino because it would provide a secure environment from which to verify files (Angelo Col. 9 lines 64-col. 10 lines 11). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ Angelo's teaching because it would set a chooser value to a value corresponding to a chooser application upon power-up. Upon power-up or reset, the computer performs the power on self-test by verifying and comparing hash value to a value stored. Loading information in to memory and execution is performed after integrity is verified.

Marino and Angelo do not explicitly teach a chooser value to a value corresponding to a chooser application;

the chooser application presenting the plurality of available applications for selection by a user;

receiving a selection of one of the presented applications to be instantiated; and

setting the chooser value to a value corresponding to the selected application;

However Downs teach setting a chooser value to a value corresponding to a chooser application (Downs Col. 31 lines 60-67, and Col. 83 lines 43-64 a user makes a selection of digital content among a plurality of digital contents and the selected value is set and music is stored in users device)

the chooser application presenting the plurality of available applications for selection by a user (Downs col. 28 lines 4-7; Content ID is used to uniquely identify content among plurality of contents);

receiving a selection of one of the presented applications to be instantiated (Downs Col. 25 lines 16-22, col. 77 lines 5-23);

setting the chooser value to a value corresponding to the selected application (Downs Col. 31 lines 60-67, and Col. 83 lines 43-64);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Downs with in the combination system of Marino and Angelo because it would securely deliver digital contents and rights management of digital assets such as print media, films games, and music over global communications networks

(Downs Col. 1 lines 61-67) by encrypting content data with a first encryption key and encrypting the first encryption key with a second encryption key (Downs Col. 3 lines 49-67).

6.3 As per claim 3, Marino teaches the processor wherein the application is selected from a banking/financial system (Marino Col. 1 lines 20-39);

Marino does not explicitly teach the application is selected from a group consisting of a digital rights management (DRM) system;

However Downs teaches the application is selected from a group consisting of a digital rights management (DRM) system (Downs Col. 19 lines 22-28);

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Downs with in the combination system of Marino and Angelo because it would prevent unauthorized copy of digital contents (Downs Col. 19 lines 21-28).

6.4 As per claim 5, Marino, Angelo, and Downs teach all the subject matter as described above. In addition Marino teaches the processor wherein the security kernel initially authenticates (Marino Col. 6 lines 48-57) a chooser application that allows a user to select from at least one available applications on the computing device (Downs Col. 31 lines 64-67, col. 78, lines 22-40). The rational for combining are the same as claim 25 above.

6.5 As per claim 8, Marino, Angelo, and Downs teach all the subject matter as described above. In addition Downs teaches the processor wherein the computing device is a portable

computing device (Downs Col. 77 lines 50-62). The rational for combining are the same as claim 25 above.

6.6 As per claim 21 and 37, Marino, Angelo, and Downs teach all the subject matter as described above. In addition Downs teaches a method (medium) wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU (Downs Col. 3 lines 48-67; encrypting an encryption key)
KMAN (KCODE)	KCODE encrypted according to KMAN (Downs Col. 3 lines 48-67; encrypting digital content)

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN (Downs Col. 16 lines 17-47; decrypting the encrypted encryption key); and

applying KMAN to KMAN (KCODE) to produce KCODE (Downs Col. 7 lines 35-64; decrypting the encrypted digital content).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Downs with in the combination system of Marino and Angelo because it would allow to authenticate and verify the integrity of the Digital Content by encrypting content data with a first encryption key, the first encryption key is encrypted with a second encrypting key (Downs Abstract, and Col. 6 lines 59-67), and

6.7 As per claim 22 and 38, Marino, Angelo, and Downs teach all the subject matter as described above. In addition Downs teaches a method (medium) wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU (Downs Col. 3 lines 48-67; encrypting an encryption key)
MAC (main body, KMAN)	message authentication code of the main body under KMAN ((Downs Col. 73 lines 24-48)
KMAN (KCODE)	KCODE encrypted according to KMAN (Downs Col. 3 lines 48-67; encrypting digital content)

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN (Downs Col. 16 lines 17-47; decrypting the encrypted encryption key);

computing MAC (main body, KMAN) (Downs Col. 16 lines 19-47);

comparing the computed MAC to MAC (main body, KMAN) from the header to determine if the code image has been changed (Downs Col. 16 lines 19-47); and

if the MACs match, applying KMAN to KMAN (KCODE) to produce KCODE (Downs Col. 16 lines 19-47).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Downs with in the combination system of Marino and Angelo because it would authenticate and verify digital content, encryption key and user request (Downs Col. 73 lines 24-47)

6.7 As per claim 23 and 39, Marino, Angelo, and Downs teach all the subject matter as described above. In addition Downs teaches a method (medium) wherein the security key of the processor is a private key of a public key--private key pair and the application is instantiated

from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key (Downs Col. 13 lines 41-48)

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises applying the security key as the private key to public key (KCODE) to produce KCODE (Downs Col. 13 lines 41-48). The rational for combining are the same as claim 21 above.

6.8 As per claim 24 and 40, Marino, Angelo, and Downs teach all the subject matter as described above. In addition Downs teaches a method (medium) wherein the security key of the processor is a private key of a public key--private key pair and the application is instantiated from a code image including a main body and a header including:

public key (HASH (main body), KCODE)	Hash of the main body and KCODE, both encrypted according to the public key (Downs Col. Lines 55-67)

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

computing HASH (main body) (Downs Col. 16 lines 19-47);

applying the private key to public key (HASH (main body), KCODE) to produce HASH (main body) and KCODE (Downs Col. 16 lines 18-40);

comparing the computed HASH to the produced HASH to determine if the code image has been changed (Downs Col. 16 lines 19-47); and

if the HASHs match, employing the produced KCODE as appropriate (Downs Col. 16 lines 19-47). The rational for combining are the same as claim 22 above.

6.9 As per claim 26 and 42, Marino, Angelo, and Downs teach all the subject matter as described above. In addition Marino teaches a method (medium) further comprising application being

authenticated by the security kernel (Marino Col. 6 lines 48-57),

the security kernel determines that the chooser value corresponds to the chooser application 72c and therefore authenticates same (Marino Col. 10 lines 5-26).

Setting a value wherein upon execution of a CPU reset (Angelo Col. 3 lines 5-40)

setting the chooser value to the value corresponding to the chooser application upon the selected (Downs Col. 31 lines 60-67, and Col. 83 lines 43-64). The rational for combining are the same as claim 25 above.

6.10 As per claim 29 and 45, Marino, Angelo, and Downs teach all the subject matter as described above. In addition Marino teaches a method (medium) wherein the security key of the processor is a symmetric key and the second security kernel is instantiated by the first security kernel from a code image including a main body and a header including:

KCPU (KMAN) KMAN	encrypted according to KCPU (Downs Col. 3 lines 48-67; encrypting an encryption key)
KMAN (KCODE)	KCODE encrypted according to KMAN (Downs Col. 3 lines 48-67; encrypting digital content)

where KCPU is a security key of the processor, KMAN is a device key independent of the security key, and KCODE is the private key of the second security kernel, and

wherein the first security kernel applies the security key to decrypt the private key of the second security kernel during instantiation thereof by:

applying KCPU to KCPU (KMAN) to produce KMAN (Downs Col. 16 lines 17-47; decrypting the encrypted first key using a second encryption key); and

applying KMAN to KMAN (KCODE) to produce KCODE (Downs Col. 7 lines 35-64; decrypting the encrypted digital content). The rational for combining are the same as claim 21 above.

6.11 As per claim 30 and 46, Marino, Angelo, and Downs teach all the subject matter as described above. In addition Marino teaches a method (medium) wherein the application is instantiated by the second security kernel from a code image including a main body and a header including:

public key (KCODE) KCODE	encrypted according to the public key (Downs Col. 13 lines 41-48)

where KCODE is the secret of the application, and

wherein the second security kernel applies the private key to decrypt the secret of the application during authentication thereof (Downs Col. 13 lines 41-48). The rational for combining are the same as claim 23 above.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 703-305-0326. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100